

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2002 年 5 月 30 日 (30.05.2002)

PCT

(10) 国際公開番号
WO 02/42920 A1

- (51) 国際特許分類: G06F 15/00, 13/00, 9/06
- (21) 国際出願番号: PCT/JP01/09779
- (22) 国際出願日: 2001 年 11 月 8 日 (08.11.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2000-356467
2000 年 11 月 22 日 (22.11.2000) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社
エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.)
[JP/JP]; 〒100-6150 東京都千代田区永田町二丁目 11
番 1 号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 山田和宏 (YA-
MADA, Kazuhiro) [JP/JP]; 〒232-0066 神奈川県横浜市
南区六ツ川一丁目 660 Kanagawa (JP). 山本正明 (YA-
MAMOTO, Masaaki) [JP/JP]; 〒235-0033 神奈川県横

浜市磯子区杉田九丁目 2-10-107 Kanagawa (JP). 平松
孝朗 (HIRAMATSU, Yoshiaki) [JP/JP]; 〒239-0805 神
奈川県横須賀市舟倉二丁目 5 番 20 号 Kanagawa (JP). 井
上恭子 (INOUE, Kyoko) [JP/JP]; 〒150-0022 東京都渋谷
区恵比寿南一丁目 19-10-302 Tokyo (JP). 大関江利子
(OOSEKI, Eriko) [JP/JP]; 〒239-0847 神奈川県横須賀
市光の丘 6-1-704 Kanagawa (JP). 徳田元紀 (TOKUDA,
Motoki) [JP/JP]; 〒239-0843 神奈川県横須賀市津久井
一丁目 22-41 シェルクレーン 2-202 Kanagawa (JP). 大
井達郎 (OOI, Tatsuro) [JP/JP]; 〒236-0031 神奈川県横
浜市金沢区六浦一丁目 21-19-307 Kanagawa (JP).

(74) 代理人: 川崎研二 (KAWASAKI, Kenji); 〒103-0027 東
京都中央区日本橋一丁目 2 番 10 号 東洋ビルディング
7 階 朝日特許事務所 Tokyo (JP).

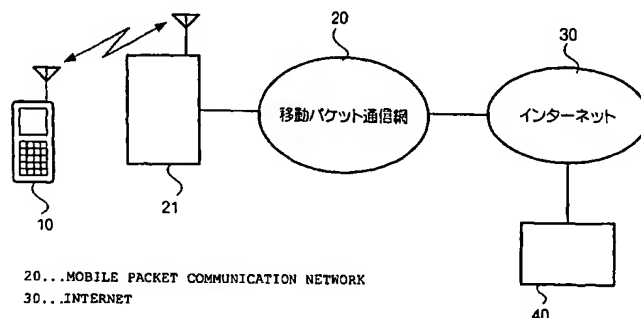
(81) 指定国 (国内): BR, CA, JP, US.

添付公開書類:
— 国際調査報告書

2 文字コード及び他の略語については、定期発行される
各 PCT ガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

(54) Title: METHOD AND DEVICE FOR MANAGING ACCESS TO NETWORK

(54) 発明の名称: ネットワークへのアクセスを管理する方法および装置



(57) Abstract: When a Java application (AP) is downloaded from a server (40), the scheme and the transmission port number used during the download by the server (40) as well as the host name of the server (40) are recorded. When the Java application (AP) accesses a resource on a network, the host name of the resource, the scheme, and the destination port number are compared with recorded host name, scheme, and transmission port number. Only if all of them agree, the network access is permitted.

[続葉有]

WO 02/42920 A1



(57) 要約:

サーバ４０からジャバアプリケーションＡＰをダウンロードする際に、サーバ４０のホスト名とともに、ジャバアプリケーションＡＰをダウンロードする際にサーバ４０が用いたスキーム及び送信ポート番号を記憶しておく。そして、ジャバアプリケーションＡＰがネットワーク上のリソースにへアクセスする場合に、アクセスしようとしてしているリソースのホスト名、スキーム及び宛先ポート番号を、記憶しているホスト名、スキーム及び送信ポート番号と比較して、これらが全て一致する場合にのみ、そのネットワークアクセスを許容する。

明細書

ネットワークへのアクセスを管理する方法および装置

5 技術分野

本発明は、ネットワーク上のリソースからダウンロードしたソフトウェアが実行される際に、当該ソフトウェアによるネットワークへのアクセスを管理するための方法および装置に関する。

10 背景技術

ネットワークに接続されたクライアント端末は、ネットワーク上のサーバにアクセスし、各種コンテンツやアプリケーションをダウンロードすることができる。

例えば、Java（登録商標）プログラミング言語で記述された「ジャバアプレット」と呼ばれるソフトウェアは、サーバのようなソースコンピュータからクライアント端末にダウンロードされ、そのクライアント端末に実装されたブラウザ上で実行されるように構成されたソフトウェアである。

このジャバアプレットは、クライアント端末側のCPUやメモリの負担を軽減するべく低容量化された小さなアプリケーションで、処理を実行する際にはネットワーク上のサーバにアクセスし、このサーバと連携しながら処理を実行するようになっている。

ところが、インターネットのようなオープンネットワークは一般に安全性が低く、そのため、このようなオープンネットワークを介して配布されるジャバアプレットは必ずしも信頼できるものではない。

そこで、不正なジャバアプレットによるネットワークアクセスを排除する必要がある。現在、次のようなアクセス制限の仕組みが提案されている。

即ち、クライアント端末は、ジャバアプレットのダウンロード元のサーバに対してのみアクセスを可能とするものである。具体的には、クライアント端末が、ジャバアプレットのダウンロード元のサーバのホスト名を、ジャバアプレットの識別情報とともに記憶しておき、このジャバアプレットがネットワークへのアクセスを行う場合には、これと対応付けて記憶しておいたホスト名以外のサーバへのアクセス

を禁止するようにしている。このアクセス制限手法は、一般に「サンドボックス」と呼ばれている。

ところで、J a v a（登録商標）プログラミング言語で記述されたソフトウェアには、上記ジャバアプレットのほかに、「ジャバアプリケーション」と呼ばれるものがある。このジャバアプリケーションは、サーバからクライアント端末にダウンロードされてもよいし、予めクライアント端末に実装されていてもよいが、その実行時には、クライアント端末内のブラウザ以外のソフトウェアと共同して作動するものである。また、このジャバアプリケーションによるネットワークへのアクセスは、上述したサンドボックスの対象とはなっておらず、ネットワーク上のいずれのサーバとも通信可能となっている。

ただし、今後は、J a v a（登録商標）に適合したネットワーク資源の構築がよりいっそう進むことが予想され、そのような状況下では、ジャバアプリケーションによるネットワークアクセスに対しても何らかの制限を設ける必要が生じてくると考えられる。

しかしながら、上述したサンドボックスをジャバアプリケーションに採用しただけでは、不正なジャバアプリケーションによるネットワークアクセスを完全に排除できるとは言い難い。なぜなら、アクセス先をダウンロード元のサーバに限定しても、通常、1個のサーバの処理内容は多岐に渡り、必ずしもユーザが意図している処理をクライアント端末がサーバに実行させるとはいえないからである。

このような背景の下、本発明は、例えばジャバアプリケーションのようなソフトウェアによるネットワークアクセスに関して、よりセキュリティを向上させることを目的とする。

発明の開示

上記課題を解決するため、本発明は、ソフトウェアによるネットワークへのアクセスを管理するアクセス管理方法であって、クライアントがネットワーク上のリソースからソフトウェアをダウンロードする際に、前記リソースが用いたスキーム及び送信ポート番号を、前記リソースのホスト名とともに記憶するステップと、ダウンロードされた前記ソフトウェアが実行されることによりネットワーク上のリソースへアクセスする場合、そのアクセス対象となるリソースのホスト名と、当該ア

クセスに用いるスキーム及び宛先ポート番号とを、前記記憶しているホスト名、スキーム及び送信ポート番号と比較するステップと、前記比較の結果、一致した場合には前記アクセスを許容する一方、一致しない場合には前記アクセスを許容しないステップとを備えることを特徴とするアクセス管理方法を提供する。この場合、前記ソフトウェアは、Java（登録商標）プログラミング言語で記述され、前記クライアントに予めインストールされているソフトウェアと共同して実行されるジャバアプリケーションでもよい。

さらに、本発明は、上記アクセス管理方法の各ステップにおいて実行される処理をコンピュータに実行させるプログラムおよびアクセスを管理するアクセス管理方法をコンピュータに実行させるプログラムを記憶したコンピュータ読み取り可能な記録媒体を提供する。

さらに、本発明は、ソフトウェアによるネットワークへのアクセスを管理するアクセス管理装置であって、クライアントがネットワーク上のリソースからソフトウェアをダウンロードする際に、前記リソースが用いたスキーム及び送信ポート番号を、前記リソースのホスト名とともに記憶する記憶手段と、ダウンロードされた前記ソフトウェアが実行されることによりネットワーク上のリソースへアクセスする場合、そのアクセス対象となるリソースのホスト名と当該アクセスに用いるスキーム及び宛先ポート番号を、前記記憶しているホスト名、スキーム及び送信ポート番号と比較する比較手段と、前記比較の結果、一致した場合には前記アクセスを許容する一方、一致しない場合には前記アクセスを許容しない制御手段とを備えることを特徴とするアクセス管理装置を提供する。

さらに、本発明は、移動通信網に收容され、該網を介してデータ通信を行う移動通信端末であって、所定のリソースから前記移動通信網を介してソフトウェアをダウンロードするダウンロード手段と、前記ソフトウェアをダウンロードする際に前記リソースが用いたスキーム及び送信ポート番号を、前記リソースのホスト名とともに記憶する記憶手段と、ダウンロードされた前記ソフトウェアが実行されることによりネットワーク上のリソースへアクセスする場合、そのアクセス対象となるリソースのホスト名と当該アクセスに用いるスキーム及び宛先ポート番号を、前記記憶しているホスト名、スキーム及び送信ポート番号と比較する比較手段と、前記比較の結果、一致した場合には前記アクセスを許容する一方、一致しない場合には前

記アクセスを許容しない制御手段とを備えることを特徴とする移動通信端末を提供する。

- 5 本発明によれば、ネットワーク上のリソースからソフトウェアをダウンロードする際に、リソースのホスト名とともに、ソフトウェアをダウンロードする際にリソースが用いたスキーム及び送信ポート番号を記憶しておき、ソフトウェアがネットワーク上のリソースへアクセスする場合に、アクセス対象となるリソースのホスト名、スキーム及び宛先ポート番号を、記憶しているホスト名、スキーム及び送信ポート番号と比較し、これが一致する場合にのみアクセスを許容するので、アクセス先がより限定される結果となり、これによりセキュリティが向上することになる。

10

図面の簡単な説明

図1は、本発明の実施形態に係るシステムの全体構成を示すブロック図である。

図2は、同実施形態における携帯電話機のハードウェア構成を示すブロック図である。

- 15 図3は、同実施形態における携帯電話機のソフトウェア構成を示す模式図である。

図4は、同実施形態における携帯電話機が備えるアクセス管理テーブルに登録されている内容の一例を示す図である。

図5は、同実施形態における携帯電話機がジャバアプリケーションをダウンロードする際の処理動作を示すフローチャートである。

- 20 図6は、同実施形態における携帯電話機のジャババーチャルマシンが、ダウンロードしたジャバアプリケーションを実行する際の処理動作を示すフローチャートである。

発明を実施するための最良の態様

- 25 以下、図面を参照しながら、本発明の実施形態を説明する。この実施形態では、クライアント端末として、無線によりデータ通信を行う携帯電話機を例に挙げて説明する。ただし、本発明は、かかる実施形態に限定されず、その技術思想の範囲内で種々の変化が可能である。

30 A：構成

まず、実施形態の構成について説明する。

(1) システム全体の構成

図1は、本発明の実施形態にかかるシステム全体の構成を示すブロック図である。同図に示すように、このシステムは、携帯電話機10、移動パケット通信網20、インターネット30及びサーバ40から構成されている。

携帯電話機10は、ユーザによって所持され、図示せぬ移動電話網の通話サービスを受けるほか、移動パケット通信網20の基地局21との間で無線通信を行って該網20のデータ通信サービスを受ける。

この携帯電話機10は、インターネット30上の各種ページをブラウジングするためのブラウザのほか、Java（登録商標）をサポートするジャババーチャルマシンを搭載しており、これにより、サーバ40からダウンロードした各種ジャバアプリケーションを実行することが可能となっている。

移動パケット通信網20は、基地局21や、図示せぬ交換局及びこれらを結ぶ通信線によって構成される。基地局21は、移動パケット通信網20の通信サービスエリア内に所定の間隔で多数設置され、各々の無線セルに在圏する携帯電話機10と無線通信を行う。

この移動パケット通信網20は、図示せぬゲートウェイを介してインターネット30に接続されており、これらのネットワーク間では双方向のデータ中継が可能である。

サーバ40は、各種データやソフトウェアを保持しており、これらをインターネット30及び移動パケット通信網20を介して携帯電話機10に提供する。

例えば、サーバ40は、携帯電話機10のブラウザを用いて参照可能なHTML（Hypertext Markup Language）形式のデータや、Java（登録商標）プログラミング言語で記述されたジャバアプリケーションを保持している。このジャバアプリケーションは、例えば、株売買等のオンライントレーディングや、ユーザのアドレス帳或いはPIM（Personal Information Manager）等の管理を行うためのソフトウェアであり、サーバ40から携帯電話機10にダウンロードされた後、携帯電話機10上でサーバ40と連携しながら実行されるようになっている。

(2) 携帯電話機 10 のハードウェア構成

次に、図 2 に示すブロック図を参照しながら、携帯電話機 10 のハードウェア構成について説明する。

同図に示すように、携帯電話機 10 は、送受信部 11、制御部 12、ユーザインタフェース部 13 及びこれらを相互に接続するバス 14 から構成される。

送受信部 11 は、図示せぬアンテナや通信制御回路からなり、移動パケット通信網 20 の基地局 21 と無線通信を行う。

ユーザインタフェース部 13 は、各種情報を表示する液晶ディスプレイ、ユーザが各種入力操作を行うためのキーパッド、ユーザが通話を行うためのマイク及びスピーカからなる。

制御部 12 は、この携帯電話機 10 の各部を制御するものであり、CPU 121、ROM 122 及び SRAM 123 から構成される。

ROM 122 には種々の制御プログラム等が格納されており、CPU 121 は、この制御プログラムを読み出して各種制御処理を実行する。ROM 122 内の制御プログラムには、携帯電話機 10 が備えるオペレーティングシステムその他、ブラウザや、後述する各種ソフトウェアが含まれる。

SRAM 123 は、CPU 121 のワークエリアとして用いられるほか、サーバ 40 から提供されるページをキャッシュしたり、サーバ 40 からダウンロードしたジャバアプリケーションを記憶する。

(3) 携帯電話機 10 のソフトウェア構成

次に、携帯電話機 10 の ROM 122 に記憶されたソフトウェアの構成について説明する。

図 3 は、携帯電話機 10 のソフトウェア構成を示す模式図である。同図に示すように、携帯電話機 10 のソフトウェアは、最下層から最上層の順に、オペレーティングシステム OS、ジャバアプリケーションマネージャ JAM、ジャババーチャルマシン KVM、ジャバアプリケーション AP によって構成される。

オペレーティングシステム OS は、周知の携帯電話機が実装するソフトウェアであり、携帯電話機 10 の基本的な処理をサポートする。

ジャバアプリケーションマネージャ JAM は、主としてジャババーチャルマシン

KVMの制御やセキュリティチェックを行うためのソフトウェアであり、例えば、
JavaアプリケーションAPが特定のリソースへのアクセスを行う際に、そのア
クセスを許可するかどうかを判断する。JavaアプリケーションマネージャJAMは、
この判断を行うために、後述するアクセス管理テーブルを備えている。

- 5 JavaバーチャルマシンKVMは、JavaアプリケーションマネージャJAMに
よる制御の下、Javaアプリケーションを実行する。このJavaバーチャルマシン
KVM及びJavaアプリケーションマネージャJAMは、オペレーティングシステ
ムOSに予め組み込まれており、これらは全てROM122内に記憶されている。

- 10 JavaアプリケーションAPは、上述したようにJava（登録商標）プログラ
ミング言語によって記述されたソフトウェアであり、サーバ40から携帯電話機1
0にダウンロードされ、SRAM123内に書き込まれて保存される。

（４）アクセス管理テーブルの構成

- 15 図4は、JavaアプリケーションマネージャJAMが備えるアクセス管理テー
ブルの記憶内容の一例を示すフォーマット図である。なお、このアクセス管理テー
ブルは、上述したSRAM123上に設けられている。

- 20 同図に示すように、このアクセス管理テーブル上には、Javaアプリケーション
APのアプリケーション識別番号に対応付けて、そのJavaアプリケーションのダ
ウンロード元となるサーバ40のURL（Uniform Resource Locator）が
記憶されている。このURLには、サーバ40のホスト名だけではなく、スキーム
及びポート番号が含まれている。ここで、スキームとは、携帯電話機10がサーバ
40と通信する際に用いたプロトコルを意味し、例えば、http（Hypertext
Transfer Protocol）、ftp（File Transfer Protocol）等がある。また、
ポート番号とは、サーバ40がJavaアプリケーションAPを携帯電話機10に送
25 信する際に用いた送信ポート番号を意味している。このポート番号には、RFC1
700によってアプリケーション毎に予め定められているウェルノウンポート番
号と、その都度動的に定められるポート番号とがある。

- 30 図4において、例えば、アプリケーション識別番号「ap0001」に対応してURL
「http://www.abc.co.jp:80」が記憶されている。これは、アプリケーショ
ン識別番号「ap0001」が示すJavaアプリケーションAPが、ホスト名

「www.abc.co.jp」のサーバ40から、ポート番号「80」及びスキーム「http」を利用してダウンロードされたことを意味している。

- 5 ジャバアプリケーションマネージャJAMは、上述したように、ジャバアプリケーションAPが特定のリソースへのアクセスを行う際に、そのアクセスを許可するかどうかをこのアクセス管理テーブルを参照して判断する。

- 10 具体的には、ジャバアプリケーションマネージャJAMは、ジャバアプリケーションAPがインターネット30上のリソースにアクセスするような場合、そのジャバアプリケーションAPのアプリケーション識別情報に対応付けられてアクセス管理テーブルに記憶されているURLに対してのみ、アクセスを許可するようになっている。

B：動作

次に、上記構成からなる実施形態の動作について説明する。

- 15 以下では、(1)ジャバアプリケーションのダウンロード処理、(2)ジャバアプリケーションの実行処理とに分けて動作説明を行う。

(1) ジャバアプリケーションのダウンロード処理

図5は、携帯電話機10によるジャバアプリケーションAPのダウンロード処理を示すフローチャートである。

- 20 同図において、携帯電話機10は、サーバ40に対して所望のジャバアプリケーションのダウンロードを要求する(ステップS1)。具体的には、携帯電話機10はまず、サーバ40が用意しているHTML形式のメニューページを自身の液晶ディスプレイに表示し、ユーザはそのメニューの中から所望のジャバアプリケーション名を選択する。これにより、そのジャバアプリケーションAPを要求するリクエストが携帯電話機10からサーバ40に送信されてダウンロード要求がなされる。

- 25 このダウンロード要求に対してサーバ40が応答することにより、携帯電話機10によるジャバアプリケーションのダウンロード処理が開始される(ステップS2)。より具体的には、ジャバアプリケーションAPのアプリケーション識別情報及びサーバ40のURLが携帯電話機10に通知された後、ジャバアプリケーションAPそのもののデータがJARファイル形式でダウンロードされる。

- 30 携帯電話機10は、サーバ40から通知されたアプリケーション識別情報及びU

R Lを、上述したアクセス管理テーブルに書込むとともに（ステップS 3）、ジャバアプリケーションAPのデータをSRAM123の所定の記憶エリアに書き込んでいく（ステップS 4）。すべてのデータがSRAM123に書き込まれたことが確認されると、同図に示す処理は終了する。

5

（2）ジャバアプリケーションの実行処理

図6は、携帯電話機10のジャババーチャルマシンKVMによるジャバアプリケーションAPの実行処理を示すフローチャートである。

ユーザの操作により所望のジャバアプリケーションの起動が指示されると、これ
10 に応じて図3に示すジャババーチャルマシンKVM上でジャバアプリケーションAPが起動され、「クラス」と呼ばれる処理実行単位毎に処理が実行されていく。

このクラス単位で図6に示すフローが開始される。同図において、まず、実行されるクラスがネットワーク上のリソースへのアクセスを要する処理であるか否かが判断される（ステップS 11）。

15 ここで、クラスがネットワークアクセスを要するものではない場合（ステップS 11；No）、ジャババーチャルマシンKVMは、そのクラスに対応する処理を実行して（ステップS 12）、同図に示す処理は終了する。

一方、クラスがネットワークアクセスを要するものである場合（ステップS 11；Yes）、ジャババーチャルマシンKVMは、そのアクセス対象となるリソースのホスト名とそのアクセスに用いるスキーム及び宛先ポート番号を、実行されて
20 いるジャバアプリケーションAPのアプリケーション識別情報に対応付けられてアクセス管理テーブル上に記憶されているホスト名、スキーム及びポート番号（送信ポート番号）と比較する（ステップS 13）。具体的には、双方のホスト名どうし、スキームどうし、そして宛先ポート番号とポート番号（送信ポート番号）とが
25 それぞれ比較される。

この結果、比較項目が全て一致した場合には（ステップS 14；Yes）、ジャババーチャルマシンKVMは、このネットワークアクセスを許容し、ジャバアプリケーションによるアクセス処理が開始される（ステップS 15）。

一方、少なくともいずれか1つの比較項目が不一致となった場合（ステップS 1
30 4；No）、ジャババーチャルマシンKVMは、このネットワークアクセスを許容

できない旨のメッセージを液晶ディスプレイに表示し（ステップS16）、同図に示す処理は終了する。

このように、サーバ40から携帯電話機10にジャバアプリケーションAPをダウンロードする際に、サーバ40のホスト名とともに、ジャバアプリケーションAPをダウンロードする際にサーバ40が用いたスキーム及び送信ポート番号を記憶しておき、このジャバアプリケーションAPがネットワーク上のリソースへアクセスする場合に、そのアクセス対象となるリソースのホスト名、スキーム及び宛先ポート番号を、記憶しているホスト名、スキーム及び送信ポート番号と比較して、これらが全て一致する場合にのみアクセスを許容する。

- 10 即ち、アクセス先をより厳格に限定することにより、セキュリティを確保するのである。

C：変形例

- 15 既述のとおり、本発明は上述した実施形態に限定されず、以下のような種々の変形が可能である。

（1）携帯電話機10の形態

- 前述の実施形態では、クライアント端末として携帯電話機を用いるものであったが、これに限定されず、他の移動通信端末であってもよい。例えば、無線機能を内蔵したPDA（Personal Digital Assistants）であってもよい。

また、移動通信端末に限らず、インターネット30に有線接続されるパーソナルコンピュータのような固定端末であってもよい。

（2）サーバ40の形態

- 25 前述の実施形態では、サーバ40はインターネット30上に設置されているが、必ずしもそのような形態に限らない。例えば、サーバ40は、移動パケット通信網20内に設けられていてもよい。

（3）プログラミング言語の形態

- 30 前述の実施形態ではJava（登録商標）を用いていたが、これに限らず、他の

プログラミング言語であってもよいことはもちろんである。

- (4) 本発明の実施の形態には、上記実施形態において開示したアクセス管理方法
5 を実行させるプログラムを電気通信回線を介して配布する形態や、そのようなプロ
 グラムをコンピュータ読み取り可能な記録媒体に記録して頒布するという形態が
 含まれる。

請求の範囲

1. ソフトウェアによるネットワークへのアクセスを管理するアクセス管理方法であって、

- 5 クライアントがネットワーク上のリソースからソフトウェアをダウンロードする際に、前記リソースが用いたスキーム及び送信ポート番号を、前記リソースのホスト名とともに記憶するステップと、

ダウンロードされた前記ソフトウェアが実行されることによりネットワーク上のリソースへアクセスする場合、そのアクセス対象となるリソースのホスト名と、

- 10 当該アクセスに用いるスキーム及び宛先ポート番号とを、前記記憶しているホスト名、スキーム及び送信ポート番号と比較するステップと、

前記比較の結果、一致した場合には前記アクセスを許容する一方、一致しない場合には前記アクセスを許容しないステップと

を備えることを特徴とするアクセス管理方法。

15

2. 請求項1記載のアクセス管理方法において、

前記ソフトウェアは、J a v a（登録商標）プログラミング言語で記述され、前記クライアントに予めインストールされているソフトウェアと共同して実行されるジャバアプリケーションであることを特徴とするアクセス管理方法。

20

3. ソフトウェアによるネットワークへのアクセスを管理するアクセス管理方法をコンピュータに実行させるプログラムであって、

クライアントがネットワーク上のリソースからソフトウェアをダウンロードする際に、前記リソースが用いたスキーム及び送信ポート番号を、前記リソースのホスト名とともに記憶する処理と、

25

ダウンロードされた前記ソフトウェアが実行されることによりネットワーク上のリソースへアクセスする場合、そのアクセス対象となるリソースのホスト名と、当該アクセスに用いるスキーム及び宛先ポート番号とを、前記記憶しているホスト名、スキーム及び送信ポート番号と比較する処理と、

- 30 前記比較の結果、一致した場合には前記アクセスを許容する一方、一致しない場

合には前記アクセスを許容しない処理と
をコンピュータに実行させるプログラム。

4. ソフトウェアによるネットワークへのアクセスを管理するアクセス管理方法を
5 コンピュータに実行させるプログラムを記憶したコンピュータ読み取り可能な記録媒体であって、

クライアントがネットワーク上のリソースからソフトウェアをダウンロードする際に、前記リソースが用いたスキーム及び送信ポート番号を、前記リソースのホスト名とともに記憶する処理と、

- 10 ダウンロードされた前記ソフトウェアが実行されることによりネットワーク上のリソースへアクセスする場合、そのアクセス対象となるリソースのホスト名と、当該アクセスに用いるスキーム及び宛先ポート番号とを、前記記憶しているホスト名、スキーム及び送信ポート番号と比較する処理と、

- 前記比較の結果、一致した場合には前記アクセスを許容する一方、一致しない場合
15 合には前記アクセスを許容しない処理と
をコンピュータに実行させるプログラムを記憶したコンピュータ読み取り可能な記録媒体。

5. ソフトウェアによるネットワークへのアクセスを管理するアクセス管理装置であって、
20 あって、

クライアントがネットワーク上のリソースからソフトウェアをダウンロードする際に、前記リソースが用いたスキーム及び送信ポート番号を、前記リソースのホスト名とともに記憶する記憶手段と、

- ダウンロードされた前記ソフトウェアが実行されることによりネットワーク上のリソースへアクセスする場合、そのアクセス対象となるリソースのホスト名と当該アクセスに用いるスキーム及び宛先ポート番号を、前記記憶しているホスト名、スキーム及び送信ポート番号と比較する比較手段と、
25 の

前記比較の結果、一致した場合には前記アクセスを許容する一方、一致しない場合には前記アクセスを許容しない制御手段と

- 30 を備えることを特徴とするアクセス管理装置。

6. 移動通信網に収容され、該網を介してデータ通信を行う移動通信端末であって、
所定のリソースから前記移動通信網を介してソフトウェアをダウンロードする
ダウンロード手段と、

- 5 前記ソフトウェアをダウンロードする際に前記リソースが用いたスキーム及び
送信ポート番号を、前記リソースのホスト名とともに記憶する記憶手段と、

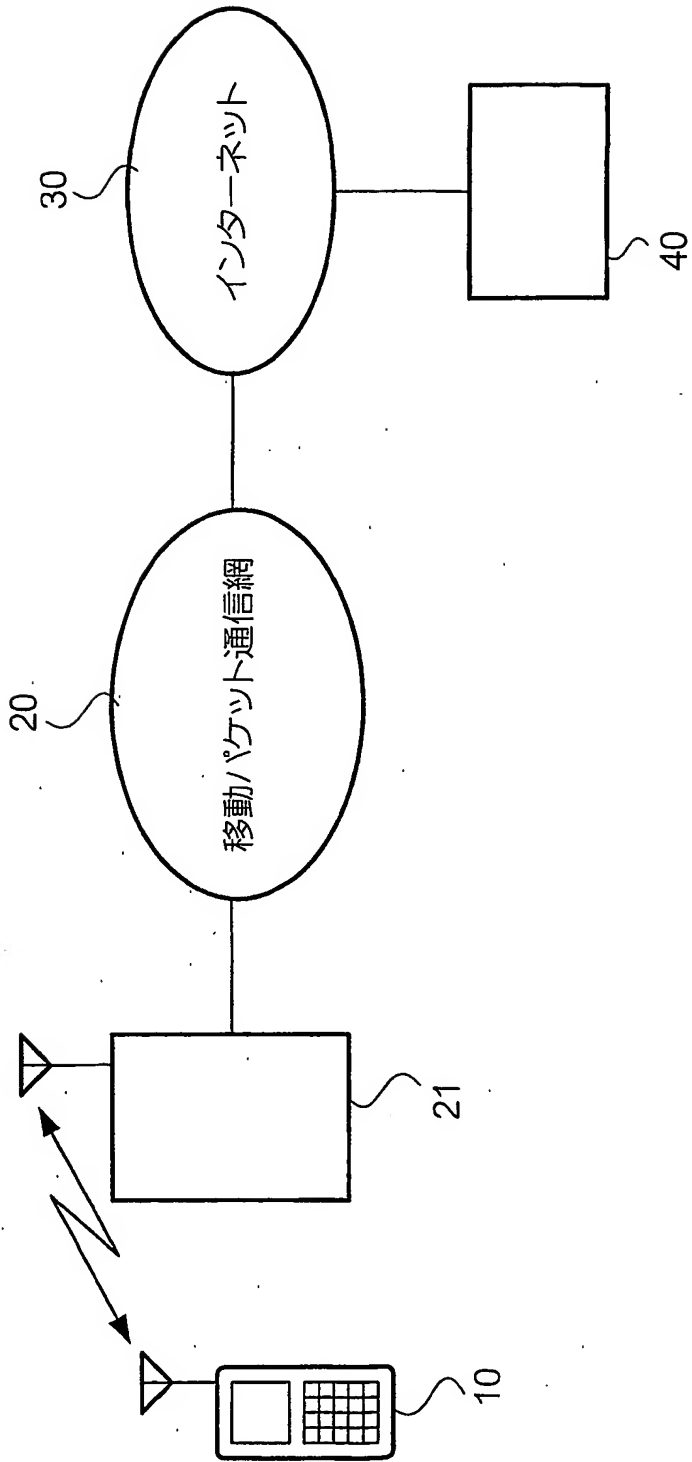
ダウンロードされた前記ソフトウェアが実行されることによりネットワーク上
のリソースへアクセスする場合、そのアクセス対象となるリソースのホスト名と当
該アクセスに用いるスキーム及び宛先ポート番号を、前記記憶しているホスト名、

- 10 スキーム及び送信ポート番号と比較する比較手段と、

前記比較の結果、一致した場合には前記アクセスを許容する一方、一致しない場
合には前記アクセスを許容しない制御手段と

を備えることを特徴とする移動通信端末。

図 1



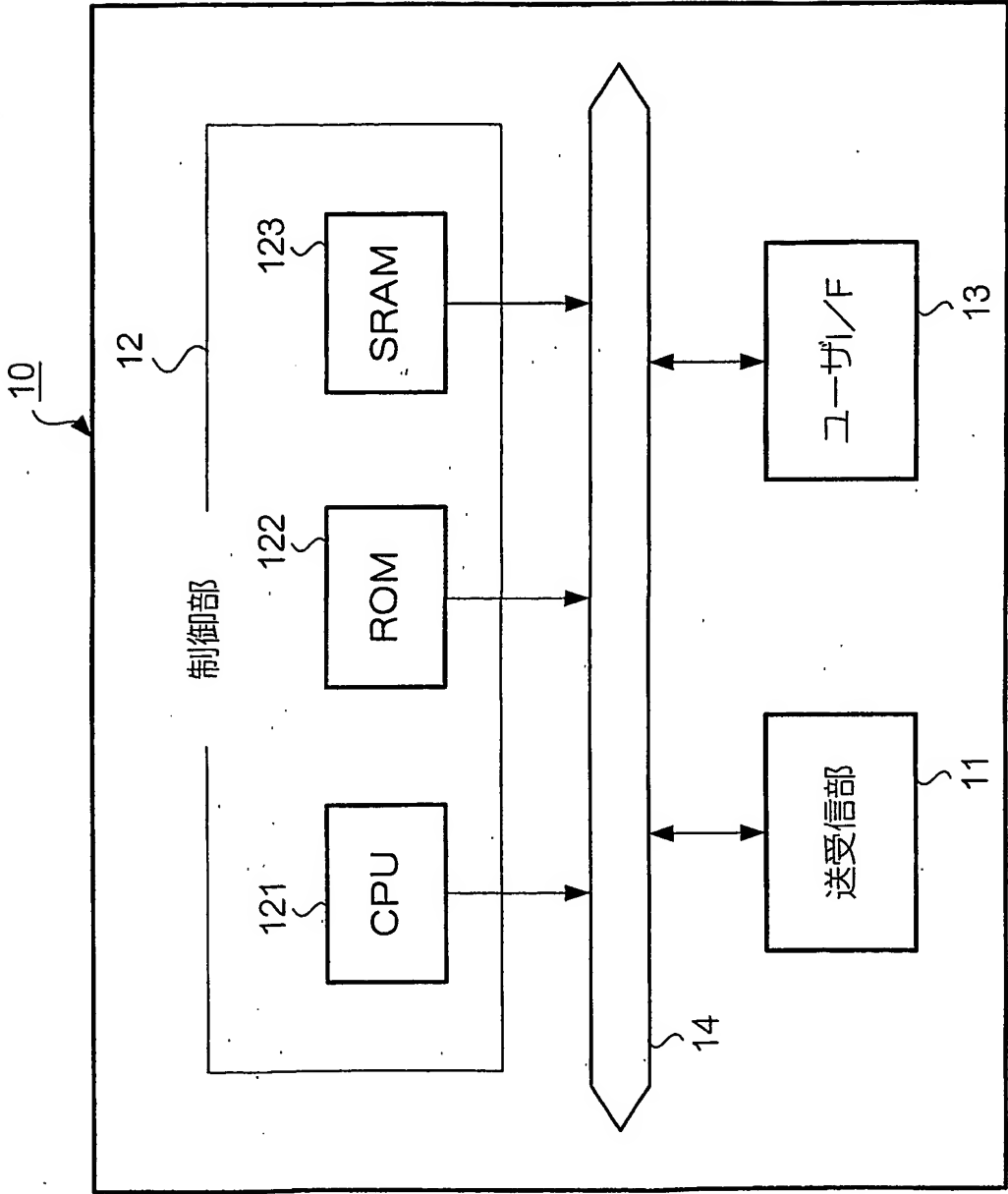


図 2

図 3

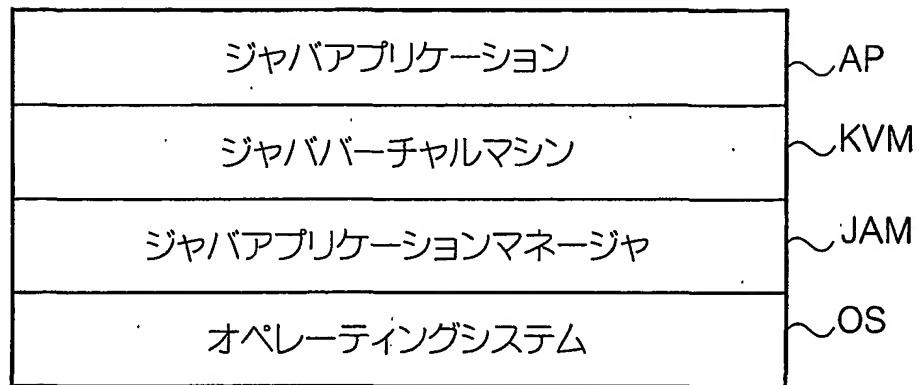


図 4

アプリケーション識別番号	URL
ap0001	http://www.abc.co.jp:80
ap0002	http://www.abc.co.jp:80
ap0035	ftp://www.abc.co.jp:21
.....
.....
.....
.....
.....

4/5

図 5

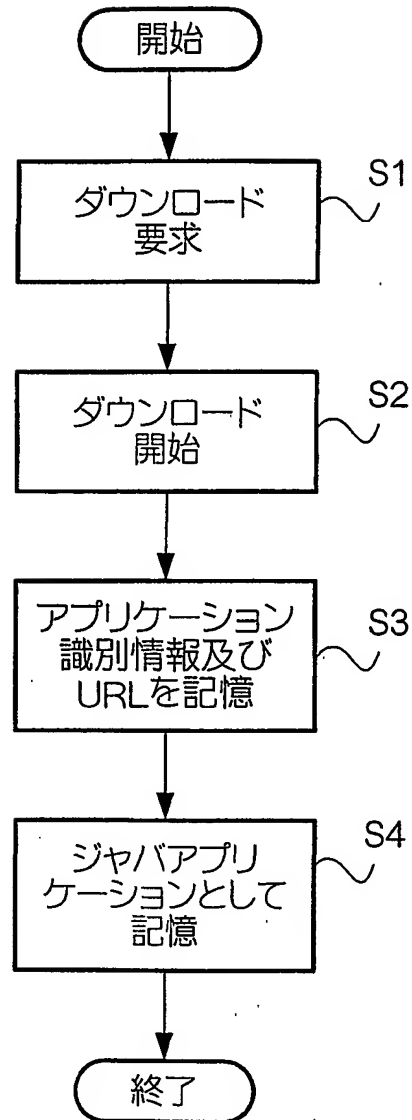
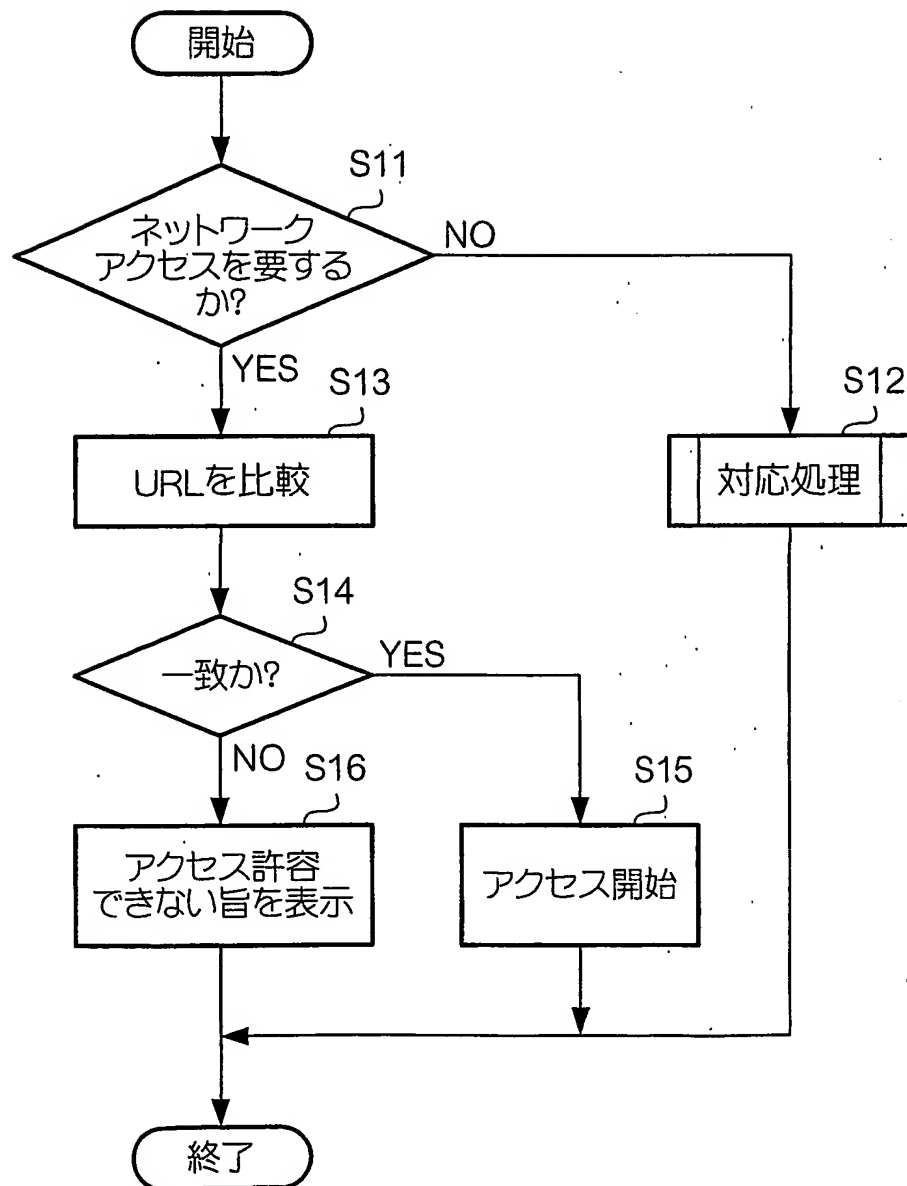


図 6



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/09779

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F15/00, G06F13/00, G06F9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F15/00, G06F13/00, G06F9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Jitsuyo Shinan Toroku Koho	1996-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Toroku Jitsuyo Shinan Koho	1994-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST DATABASE (JOIS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-45228 A (International Business Machines Corporation), 16 February, 1999 (16.02.1999), description, Par. No. [0013] & US 5987523 A & CN 1210308 A	1-6
A	Teruo NAKAMURA, "Kigyo User no tame no Java Nyumon (12kai) Network kara no kougeki wo fusegu Security Kinou no Gaiyo", Nikkei Computer, 14 September, 1998 (14.09.1998), No.452, pages 180 to 182	1-6
A	'Default Policy Implementation and Policy File Syntax'. Java2 SDK, Standard Edition Documentation, [online]. Sun Microsystems Inc., 30 October, 1998 (30.10.1998), [retrieved on: 18 January, 2002 (18.01.2002)]. Retrieved from the Internet: <URL:http://java.sun.com/j2se/1.3/docs/guide/security/ PolicyFiles.html>	1-6



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
18 January, 2002 (18.01.02)Date of mailing of the international search report
29 January, 2002 (29.01.02)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/09779

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Ryo NEYAMA, et al., "WWW jou de Koukai Kanona Bunsan Ongaku Joho System ; download shita Java Applet no tame no Anzen na Local Tsushin Houhou", Nippon Software Kagakukai, Dai 14kai Taikai Ronbunshuu, 02 October 1997 (02.10.1997), pages 185 to 188	1-6

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl ⁷ G06F15/00, G06F13/00, G06F9/06		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl ⁷ G06F15/00, G06F13/00, G06F9/06		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1926-1996年 日本国公開実用新案公報 1971-2002年 日本国実用新案登録公報 1996-2002年 日本国登録実用新案公報 1994-2002年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
JICSTデータベース (JOIS)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 11-45228 A (インターナショナル・ビジネス・マ シーンズ・コーポレーション) 1999.02.16, 明細書第 13段落 & US 5987523 A & CN 1210308 A	1-6
A	中村輝雄, 企業ユーザーのためのJava入門 (12回) ネット ワークからの攻撃を防ぐセキュリティ機能の概要, 日経コンピュ ータ, 1998.09.14, 第452号, p. 180-p. 182	1-6
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	国際調査報告の発送日	
18.01.02	29.01.02	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 宮司 卓佳 電話番号 03-3581-1101 内線 3545	

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	'Default Policy Implementation and Policy File Syntax'. Java2 SDK, Standard Edition Documentation[online]. Sun Microsystems Inc. 1998. 10. 30[retrieved on 2002. 01. 18]. Retrieved from the Internet:< URL:http://java.sun.com/j2se/1.3/docs/guide/security/PolicyFiles.html>	1-6
A	根山亮他, WWW上で公開可能な分散音楽情報システム ーダウンロードしたJavaアプレットのための安全なローカル通信方法ー, 日本ソフトウェア科学会第14回大会論文集, 1997. 10. 02, p. 185-p. 188	1-6